DOI:10.13878/j.cnki.jnuist.2019.05.012

刘帅[1,2,3] 戚荣鑫[1] 董昳晖[1] 冯孟[1] 苗田田[1] 蒋玲红[1]

一种基于区块链和边缘计算的物联网方案

摘要

物联网设备资源受限,需要使用外部资源,而集中式的云方案恰好可以为物联网提供充足的计算存储资源.但是受制于网络带宽等因素,云不能及时地处理大量的数据.云方案采用静态密码的验证和明文存储的机制,也存在着安全性问题.区块链技术的兴起,为解决物联网安全问题带来了新思路.边缘计算缩短了数据处理距离,增强了实时性.因此,本文将使用这两项技术,解决目前物联网中的问题.

关键词

区块链;物联网;边缘计算;安全

中图分类号 TP391

文献标志码 A

收稿日期 2019-07-28

资助项目 国家自然科学基金(61922045,U1836115,61672295);江苏省自然科学基金(BK20181408);密码科学技术国家重点实验室项目(MMKFKT201830);网络与交换技术国家重点实验室(北京邮电大学)开放课题(SKLNST-2019-2-02);鹏城实验室网络空间安全研究中心(PCL2018KP004)

作者简介

刘帅,男,硕士生,研究方向为网络与信息安全.shuailiu2019@126.com

1 南京信息工程大学 计算机与软件学院,南京,210044

2 鹏城实验室网络空间安全研究中心,深圳,518000

3 密码学国家重点实验室,北京,100878

0 引言

随着传感器、无线通信、数据分析处理等技术的快速发展,物联网设备趋于微型化、廉价化[1].从而,在家庭、教育、交通等领域应用物联网技术解决问题成为了可能.最初的物联网设备处理的数据量很少,可以使用有限的资源完成处理任务.然而,当物联网技术广泛应用于家庭电器、交通控制等的时候,产生的数据量越来越大.从异构的物联网中提取有价值的信息越来越困难.2010 年,Zhao[2]认为云计算为解决物联网数据处理提供了新的机会.2014 年,Biswas 等[3]认为云提供强大资源的同时,还存在异构连接、动态管理等挑战亟待解决.2015 年,Farris 等[4]通过融合边缘计算和云计算,使用一种联合机制解决了异构网络连接云的问题.2016 年,Shi 等[5]认可了基于云的物联网方案,指出了基于云的方案在处理交通信息等突发性强、实时性要求高事件的不足,并认为边缘计算可以解决这类事件.

物联网连接到因特网后,面临的安全威胁也越来越多.Sharmeen 等[6]指出了恶意攻击者侵入物联网的行为,恶意攻击者绕过授权直接访问了物联网内部数据.基于云的中心化方案,很难保证大量分散的物联网设备安全.物联网设备这种多节点、分布式的结构和比特币[7]有许多相似的特征,使用区块链技术解决安全问题成为了可能.Wu 等[8]提出了一个新的基于区块链技术的双因素安全方案,保证了智能设备数据安全.Christidis 等[9]指出使用了结合智能合约的区块链技术可以应用于物联网,而且智能合约可以为物联网提供一个不可信环境的安全.

本文旨在提出一个严格的访问控制机制,规范内网物联网设备和外网用户行为,保障物联网系统安全.

1 相关技术

1.1 区块链

2008 年,中本聪[7]在密码学论坛发表的论文,完整阐述比特币原理及区块链技术.区块链由区块和链两部分构成,包含了交易数据永久存储的数据单元就是区块,而按照时间先后顺序连接的时间戳就是链.所以,有人认为区块链是按时间先后顺序记录,通过共识机制由网络内的节点共同维护,不可篡改的分布式账本.区块的结构分为区块头和区块体两部分.区块头包含了区块自身的特征信息,如头哈希、

父哈希、时间戳、区块交易数量、区块大小等,其中的头哈希值是最关键的一个信息,总是与它连接的下一个区块父哈希值相同,如图 1 所示.区块中的区块体包含了经过验证的,区块创建过程中发生的所有交易事件记录信息,如表 1 所示是我们将使用的区块体示例.只要新生成的区块生成并添加到区块链尾部,这个区块内的数据将不能被删除或更改,确保了数据的不可篡改性.

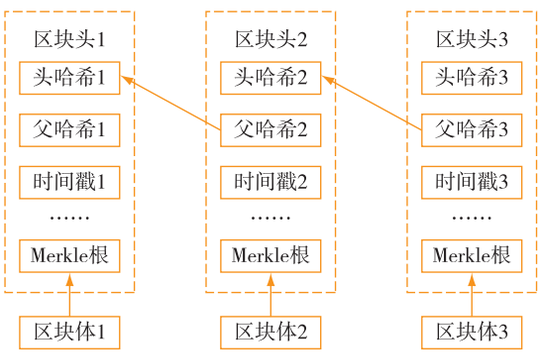


图 1　区块链结构

Fig. 1　Blockchain architecture

表 1　区块体中的事件记录

Table 1　Event logging in the block body

编号	操作/事件	Merkle 根	状态
1	存储	1	拒绝
2	访问	2	允许
3	查询	3	允许

根据区块链节点的范围分布,可以将区块链分为公有链、私有链和联盟链.公有链完全对外公开,任何人都可以直接访问区块链,不需要授权.私有链是某个组织建立的,只有特定的授权用户可以访问.联盟链是公有链和私有链的混合,只有加入联盟的用户可以访问.考虑到公有链在可靠性和隐私安全性等方面存在问题,而联盟链也因为规模较大部署起来比较困难,我们选择了规模较小的私有区块链记录存储等事件信息.也因为私有区块链是部署在本地平台,可以认为初始的区块链是安全可靠的.

1.2　边缘计算

边缘计算是在网络边缘,也就是靠近数据源附近对数据进行处理.与按需服务将数据发送到云端处理的云计算不同,边缘计算强调的是在边缘对数据处理.举个例子,智能家居里的网关就可以被认为是一个边缘,边缘计算希望在家庭网关这个边缘对数据处理.当然,如果数据量过大,边缘节点不能及时或无法完整处理,边缘节点必须依靠云完成处理任务,边缘节点将负责简单的预处理.我们的方案认为,部署的边缘节点计算和处理能力可以满足物联网设备处理需求.

2　基于区块链和边缘计算的物联网系统框架

传统的集中式管理模式是非常脆弱的,只要中心节点被破坏掉,整个物联网服务将会陷入瘫痪.因此,我们将构建一个分散监管的系统.我们的物联网系统框架如图 2 所示.这个框架包括了 4 层:感知层、边缘层、数据存储层、应用层.感知层、边缘层和数据存储层共同构成了内网.内网负责收集、存储、分析处理数据,而应用层构成的外网利用内网的数据为用户提供各类服务.

2.1　感知层

感知层包含了各类传感器节点.我们通过这些传感器,可以获得温度、湿度、气压、光照、压力之类的信息.这些传感器资源受限,只可以完成简单的数据处理任务.但他们可以将复杂的计算任务转移给边缘设备,请求边缘设备完成处理,并接收处理结果

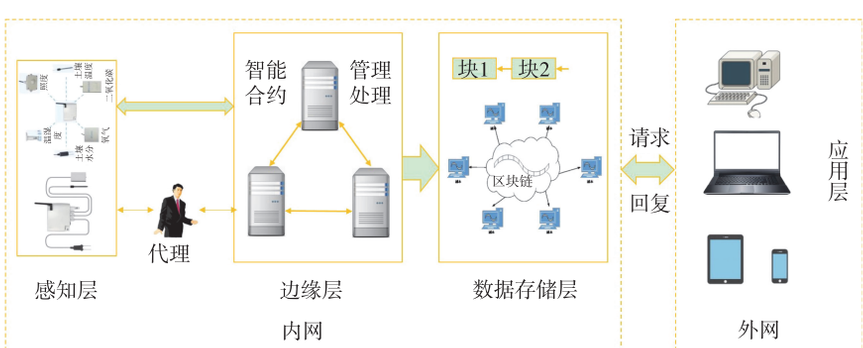


图 2　物联网系统框架

Fig. 2　IoT system framework

完成各类响应.

代理是具有较强通信和计算能力的设备,它们的任务是帮助通信能力弱的节点或者通信需求低的节点与边缘设备及上层通信.而通信能力强的传感器节点并不需要代理,它们直接与边缘设备层通信.

2.2 边缘层

运行在边缘节点上的智能合约构成了边缘层.智能合约是预先编写与部署的电子合约,包含了两个功能模块.一个功能模块是负责管理物联网设备和用户可信程度的积分系统,另一个功能模块是负责分析物联网设备行为并给出处理的规则.

管理处理是边缘设备依托于智能合约实现的.当物联网设备发出注册、使用资源等请求时,将会自动执行智能合约,根据预定义的规则处理物联网设备的请求.

2.3 数据存储层

需要存储数据时,将会自动执行智能合约.首先,智能合约会使用椭圆曲线密码算法对数据进行加密,加密使用的算法和对应解密的私钥是智能合约自行选择的,并且不会泄露给其他设备或用户.然后,智能合约会将执行的存储事件记录到区块链的块中.最后,物联网设备的各类数据经过智能合约处理,将存储在边缘设备的存储硬件.此外,如访问、查询等其他的活动事件也会被记录在块中.

2.4 应用层

应用层是一个为用户提供各类服务的平台,也是访问物联网数据的接口.用户向平台发出服务请求,平台对用户的身份进行验证,平台将通过验证的用户请求发送给边缘层的智能合约.智能合约收到用户的请求后,首先查询用户的可信程度积分,然后判断请求合理性再决定是否提供服务,并反馈给应用层.应用层对用户的验证,不仅是验证用户身份,还验证用户的请求合理性.这个验证过程可以有效的减少不合理甚至恶意的行为,减少智能合约处理的信息量,避免浪费系统资源.

3 数据处理与用户访问

物联网面临着入侵、DoS 等攻击行为.为了物联网安全,我们在容易受到安全威胁的边缘层和应用层,设计了安全保护机制.

3.1 数据处理

为了避免物联网设备窃取和滥用边缘节点的资源,我们设计了防御机制.

物联网中的设备都会直接或间接在边缘层注册,如图 3 所示.通信能力强的物联网设备可以直接向边缘层注册,而通信能力弱的将由代理管理,代理向边缘层注册.边缘层的智能合约收到注册请求后,为注册设备生成身份信息并绑定一个信用积分.这个信用积分是智能合约根据设备类型、执行的功能等因素,给予设备的一个初始分.智能合约会周期性地根据这个设备的行为事件做出评价,决定增加或减少可信积分.当可信积分减少到一个阈值时,智能合约将认为该设备是恶意设备,拒绝为其提供服务并反馈给应用层.

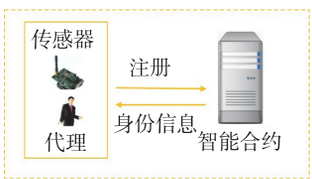


图 3 物联网设备注册

Fig. 3 IoT devices registration

为了提高响应效率,简化了认证物联网设备的流程.请求处理数据的物联网设备将验证信息嵌入在数据中,发送给边缘层.然后,智能合约检查验证信息并查看绑定可信积分.验证通过后,智能合约根据可信度分配资源处理收到的数据.处理完成后,触发智能合约的管理规则,判断做出处理策略.如果数据需要被存储,将会放入缓存中.当达到一定数量时,智能合约会使用一个比较算法计算特征值,将结果和设定的值比较,完成工作量证明(Proof of Work,PoW).计算值符合要求后,会将缓存中的数据用选定的椭圆曲线加密算法加密,然后存入数据库中(图 4).同时,智能合约将会为处理、存储的操作生成一个块记录,加入到区块链中.然后,将新加入的块记录广播给其他的边缘节点,这些节点上的智能合约再一次验证块记录并添加到节点上的区块链中.在设备通过验证的一定时间内,再一次的处理、存储、访问操作不需要验证,智能合约可以直接做出响应.而超过这个预时间后,需要再次执行验证流程.

被简化的认证流程,可以减少响应的时间,帮助时延要求高的设备处理和决策,但也降低了安全性.因此,可以采取一种动态更新设备验证信息的机制,在一定的周期内动态更新一些设备密钥等验证信息,避免一些安全攻击.智能合约也会周期性地评估设备行为,一些恶意设备的行为可以被发现,扣除设

备信用积分作为惩罚,拒绝这些设备服务请求.此外,因为物联网设备和边缘节点位于内网中,通过限制外网的访问,可以避免来自外部的攻击.通过这些措施,可以有效控制安全威胁.



图 4 数据处理与存储

Fig. 4 Data processing and data storage

3.2 用户访问

外网中对应用层的服务访问与内网的访问流程有些相似,以查询数据为例.首先,用户向应用层申请查询数据服务.然后,应用层根据请求用户的身份,向边缘层请求查询该身份绑定的可信积分.边缘层将查询到的可信情况反馈给应用层.应用层判定用户可信后,会进一步和用户交互,验证用户的合法性.验证通过后,应用层的平台,向边缘层发出查询数据的请求.边缘层进行一些处理后,将解密的数据转交给应用平台.应用平台使用用户的公钥加密数据后,将加密的数据发送给用户.最后,用户使用私钥解密数据,获得查询的数据,如图 5 所示.

同内网中的数据访问类似,在限定的时间内,用户再次访问请求可以被直接处理,不需要再次验证.而超过限定的时间,需要再次执行验证机制.此外,我们的验证机制还可以抵御 DoS 这类攻击.为了抵抗被恶意盗用的用户攻击,使用智能合约周期性地评估用户行为,调整用户的可信积分.当这个可信积分降低到一个阈值时,应用平台将拒绝这个用户的服务请求.



图 5 用户访问流程

Fig. 5 User access flowchart

3.3 新区块的生成

不论是物联网设备还是用户的访问,每一次关于数据的操作,都会产生一个记录添加到区块体中,如图 6 所示.当块记录达到上限时,智能合约会帮助数据存储层生成一个新的区块添加到数据存储层,由新的区块继续记录访问事件.这个新的区块生成后,会向其他边缘节点同步,保持区块内容一致.

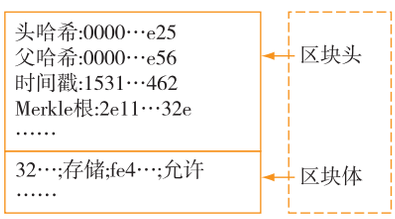


图 6 区块记录图

Fig. 6 Block record graph

4 安全性

保密性、完整性和可用性是一个系统框架最基本的需求.也就是指只有经过验证授权的用户可以访问系统信息,系统接收和发送的信息是没有更改的完整的,系统提供的数据和服务是可以被合法用户访问和使用的.参考林果园等[10]关于云计算访问控制安全的安全模型,我们认为严格控制上层访问下层并拒绝上层修改下层数据,是一个很有效的安全策略.

5 评估

本文方案和基于云的物联网方案不同.表 2 给出了一些性能上的评估.本文方案在访问控制和实时性方面优于基于云的物联网方案,而这个优势正是通过区块链和边缘计算技术实现的.

表 2 性能比较

Table 2 Comparison in the properties

性质	基于云的方案	本文方案
访问控制方式	静态的密码	动态密码、可信分
存储方式	明文	密文
安全机制	静态的密码	可信分、动态密码、工作量证明
资源数量	多	中等
实时性	一般	强
规模	大	中等

6 讨论

本文提出了一种基于区块链和边缘计算的物联网方案.通过分析现有物联网技术和方案,发现了现有方案的不足以及物联网和比特币结构的相似性.

同时,参考了基于云方案的安全模型,总结出严格控制上层访问下层并禁止篡改下层数据的控制策略.因此,我们使用了区块链技术,用区块链记录系统内操作、用户和设备行为,用唯一绑定的可信分控制用户和物联网设备行为,保障系统安全.此外,边缘计算技术为我们处理物联网数据和部署区块链提供了可靠平台.因为区块链工作量证明的安全机制占用了大量计算资源,将造成短期内资源不足.而这个工作不是该研究的重点,所以本方案没有做进一步的研究,仅增加了工作量证明的间隔.

参考文献

References

[1] Chaudhary M H, Scheers B. Software-defined wireless communications and positioning device for IoT development[C]// International Conference on Military Communications and Information Systems, IEEE, 2016, DOI:10.1109/ICMCIS.2016.7496555

[2] Zhao F. Sensors meet the cloud: planetary-scale distributed sensing and decision making[C]//9th IEEE International Conference on Cognitive Informatics, IEEE, 2010, DOI:10.1109/COGINF.2010.5599715

[3] Biswas A R, Giaffreda R. IoT and cloud convergence: opportunities and challenges[C]// IEEE World Forum on Internet of Things (WF-IoT), IEEE, 2014, DOI: 10.1109/WF-IoT.2014.6803194

[4] Farris I, Militano L, Nitti M, et al. Federated edge-assisted mobile clouds for service provisioning in heterogeneous IoT environments[C]// IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, DOI: 10.1109/WF-IoT.2015.7389120

[5] Shi W S, Cao J, Zhang Q, et al. Edge computing: vision and challenges[J]. IEEE Internet of Things Journal, 2016, 3(5): 637-646

[6] Sharmeen S, Huda S, Abawajy J H, et al. Malware threats and detection for industrial mobile-IoT networks[J]. IEEE Access, 2018, 6: 15941-15957

[7] Nakamoto S. Bitsoin: A peer-to-peer electronic cash system[EB/OL]. [2019-06-20] https://bitcoin.org/bitcoin.pdf

[8] Wu L F, Du X J, Wang W, et al. An out-of-band authentication scheme for Internet of Things using blockchain technology[C]// International Conference on Computing, Networking and Communications (ICNC), IEEE, 2018, DOI:10.1109/ICCNC.2018.8390280

[9] Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303

[10] 林果园,贺珊,黄皓,等.基于行为的云计算访问控制安全模型[J].通信学报,2012,33(3):59-66
LIN Guoyuan, HE Shan, HUANG Hao, et al. Access control security model based on behavior in cloud computing environment[J]. Journal on Communications, 2012, 33(3): 59-66

A solution for internet of things based on blockchain and edge computing

LIU Shuai[1,2,3] QI Rongxin[1] DONG Yihui[1] FENG Meng[1] MIAO Tiantian[1] JIANG Linghong[1]

1 School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing 210044

2 Cyberspace Security Research Center, Pengcheng Laboratory, Shenzhen 518000

3 State Key Laboratory of Cryptology, Beijing 100878

Abstract The resource of the internet of things (IoT) devices is limited and external resources are needed. While a centralized cloud solution can provide sufficient computing and storage resources for the internet of things. However, the cloud cannot process large amounts of data promptly, due to some factors such as network bandwidth. The scheme based on cloud uses static password authentication and plaintext storage mechanism, thus there are some security problems. The emerging technology of blockchain brings a new idea to solve the security problems of the internet of things. And edge computing shortens the distance of data processing and enhances the real-time performance. Therefore, this paper will use these two technologies to solve the current problems in the internet of things.

Key words blockchain; internet of things (IoT); edge computing; security